Chương 4 Hệ thống thanh toán điện tử

1. Tổng quan
2. Hệ thống thanh toán điện tử đặc trưng
3. Thanh toán offline và online
4. Hệ thống ghi nợ và Hệ thống tín dụng
5. Thanh toán Macro và Micro
6. Công cụ thanh toán
7. Thanh toán sử dụng thẻ tín dụng
8. Tiền điện tử (E-Money)
9. Séc điện tử (E-checks)
10. Ví điện tử (E-wallet)
11. Thẻ thông minh (Smart card)
12. Tiền mặt điện tử (E-cash)

1

1. Tổng quan về hệ thống E-payment

- Thanh toán điện tử (**E-payment)** là khâu hoàn thiện quy trình kinh doanh và việc đẩy nhanh quá trình quay vòng vốn đây là vấn đề quan trọng đối với các doanh nghiệp.
- Thanh toán điện tử là một trong các vấn đề cốt lõi của thương mại điện tử. Nếu thiếu hạ tầng thanh toán thì chưa thể có thương mại điện tử hoàn chỉnh

2

1. Tổng quan về hệ thống E-payment

- Khái niệm về thanh toán điện tử
  - Theo nghĩa rộng thanh toán điện tử là thanh toán tiền thông qua các thông điệp điện tử thay cho việc trao tay tiền mặt.
  - Theo nghĩa hẹp thanh toán điện tử là việc trả tiền và nhận tiền hàng cho các hàng hóa dịch vụ được mua bán trên mạng

3

1. Tổng quan về hệ thống E-payment

- Hệ thống E-payment được phát triển từ hệ thống thanh toán truyền thống
  - Hai hệ thống trên có nhiều điểm chung
  - Hệ thống thanh toán điện tử có tính năng vượt trội hơn hẳn, với những kĩ thuật bảo mật tiên tiến mà hệ thống thanh toán truyền thống không có được
    - ⇨ Thông qua phương tiện điện tử, loại bỏ hầu hết việc giao nhận giấy tờ và việc ký truyền thống thay vào đó là phương pháp xác thực mới.

4

1. Tổng quan về hệ thống E-payment

- Lợi ích
  - Tiết kiệm chi phí và tạo thuận lợi cho các bên giao dịch
  - Giao dịch bằng phương tiện điện tử nhanh hơn nhiều so với truyền thống
  - Các bên có thể tiến hành giao dịch khi ở cách xa nhau, không bị giới hạn bởi không gian địa lý.
- -> Thanh toán điện tử là xu thế tất yếu, cùng với TMĐT, thanh toán điện tử sẽ góp phần thúc đẩy sự cạnh tranh giữa các doanh nghiệp để thu được nhiều lợi ích nhất.

5

1. Tổng quan về hệ thống E-payment

- Trở ngại
  - Tập quán tiêu dùng, nhận thức về thanh toán điện tử là một trở ngại lớn
  - Cơ sở hạ tầng, điểm chấp nhận thanh toán là yếu tố quyết định sự thành công của thanh toán điện tử
    - Ở VN cơ sở hạ tầng còn đầu tư theo từng dự án, từng doanh nghiệp, ngân hàng thiếu tính đồng bộ và thống nhất, ít điểm chấp nhận thanh toán điện tử
  - Lo ngại về sự an toàn trong giao dịch điện tử

6

1. Tổng quan về hệ thống E-payment

- Các phương thức thanh toán trực tuyến phổ biến hiện nay
  - Thẻ thanh toán
  - Ví điện tử
  - Tiền điện tử
  - Thanh toán qua điện thoại di động
  - Thanh toán điện tử tại các ki ốt bán hàng
  - Séc điện tử
  - Thẻ mua hàng
  - Thẻ thông minh
  - Chuyển tiền điện tử (EFT- Electronic Fund Tranfering)

7

1. Tổng quan về hệ thống E-payment

- Một hệ thống thanh toán điện tử bao gồm các loại dịch vụ mạng cung cấp việc trao đổi tiền cho hàng hóa và dịch vụ:
  - Hàng hóa dịch vụ: sách báo, đĩa CD…
  - Hàng hóa điện tử: Tài liệu điện tử, hình ảnh, file nhạc
  - Dịch vụ truyền thống: đặt phòng khách sạn, đặt vé máy bay
  - Dịch vụ điện tử: ví dụ như các phân tích thị trường tài chính dưới hình thức điện tử

8

2. Hệ thống E-payment đặc trưng

- Nhà cung cấp dịch vụ thực thi một cổng thanh toán (run a payment gateway)
  - Truy cập từ mạng công cộng (Internet) và từ mạng lưới thanh toán bù trừ liên ngân hàng cá nhân
  - Đóng vai trò như một trung gian giữa hạ tầng của phương thức thanh toán truyền thống với hạ tầng của phương thức thanh toán điện tử

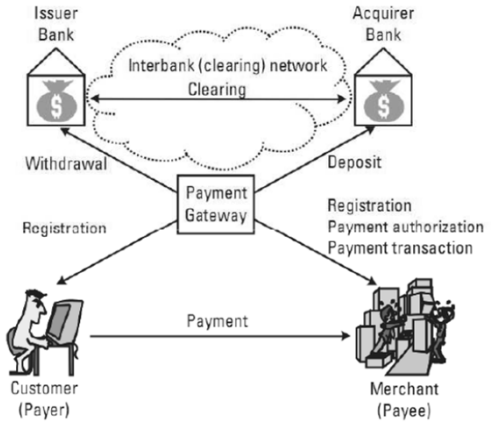
9

2. Hệ thống E-payment đặc trưng (Tiếp)

- Để tham gia, khách hàng và người bán phải
  - Đăng ký với nhà cung cấp dịch vụ thanh toán tương ứng
  - Mỗi người có một tài khoản ngân hàng tại một ngân hàng được kết nối với mạng thanh toán bù trừ
  - Ngân hàng của khách hàng được gọi là ngân hàng phát hành (Issuer bank), trên thực tế là ngân hàng phát hành công cụ thanh toán (ví dụ, thẻ ghi nợ hoặc thẻ tín dụng) mà khách hàng sử dụng để thanh toán
  - Ngân hàng thanh toán (Acquirer bank) yêu cầu các dữ liệu, hồ sơ thanh toán (giấy, phiếu thu tiền hoặc dữ liệu điện tử) từ người bán

10

2. Hệ thống E-payment đặc trưng (Tiếp)



11

2. Hệ thống E-payment đặc trưng (Tiếp)

- Khi thực hiện mua hàng hóa/ dịch vụ, khách hàng (Customer C) chi trả 1 khoản tiền cho người bán (Merchant M) thông qua thẻ ghi nợ/ tín dụng
  - Trước khi thực hiện việc cung ứng hàng hóa/dịch vụ, M sẽ hỏi cổng thanh toán (Gateway G) để xác thực khách hàng C và công cụ thanh toán của người này (số thẻ…), G liên hệ với ngân hàng phát hành để kiểm tra
  - Nếu tất cả là hợp lệ, tiền sẽ được trừ (hoặc ghi nợ) vào tài khoản của khách hàng C và gửi (hoặc ghi có) vào tài khoản của người bán M

12

2. Hệ thống E-payment đặc trưng (Tiếp)

- Cổng thanh toán G thông báo thanh toán thành công cho người bán M, M cung cấp các sản phẩm đã đặt cho khách hàng C
- Trong một vài trường hợp, để giảm chi phí dịch vụ, việc giao hàng có thể được thực hiện trước hoạt động cấp phép/giao dịch thanh toán

13

3. Hệ thống Off-line và Hệ thống On-line

a. Hệ thống Off-line

- Không có kết nối hiện tại giữa khách hàng/người bán tới ngân hàng tương ứng của họ
  - Người bán M không thể xác thực khách hàng C với ngân hàng phát hành
  - Khó thực hiện việc ngăn cản khách hàng C sử dụng nhiều tiền hơn thực sở hữu của họ
  - **Hầu hết các hệ thống thanh toán đề xuất trên Internet là trực tuyến**

14

3. Hệ thống Off-line và On-line (Tiếp)

b. Hệ thống On-line

- Yêu cầu sự hiện diện trực tuyến của máy chủ cấp phép, có thể là 1 phần của tổ chức ngân hàng phát hành hay ngân hàng thanh toán
- Đòi hỏi nhiều giao tiếp hơn nhưng cũng phải an toàn hơn so với hệ thống off-line
- **Tuy nhiên, hệ thống off-line vẫn khả quan, ví dụ trong hệ thống tiền mặt điện tử**

15

4. Hệ thống tín dụng và ghi nợ

- Trong hệ thống thanh toán tín dụng (ví dụ: thẻ tín dụng), những chi phí được gửi vào tài khoản của người trả tiền
  - Đối tượng thanh toán tiến hành chi trả sau số tiền tích lũy cho các dịch vụ thanh toán
- Trong hệ thống thanh toán ghi nợ, ví dụ: thẻ ghi nợ, séc
  - Tài khoản của người trả tiền được ghi nợ ngay lập tức, có nghĩa là, ngay khi giao dịch được xử lý

16

5. Thanh toán Macro và Micro

- Macro: lượng tiền tương đối lớn có thể được trao đổi
- Micro: các khoản thanh toán nhỏ, ví dụ, nhỏ hơn 5 euro
- Số lượng tiền đóng một vai trò quan trọng trong việc thiết kế hệ thống và các chính sách bảo mật của nó
  - Không có ý nghĩa thực tiễn khi thực hiện các giao thức bảo mật đắt tiền để bảo vệ những đồng e-coin có giá trị thấp
  - Trong trường hợp này, nên thay bằng việc ngăn chặn các cuộc tấn công quy mô lớn, trong đó số lượng lớn các đồng tiền có thể là giả mạo hoặc bị đánh cắp

17

6. Công cụ thanh toán

- Hai nhóm công cụ chính
  - Cash-like: tiền được lấy từ tài khoản trước khi thanh toán
    - ⇨ Đối tượng nộp tiền rút một số tiền nhất định (tiền giấy, tiền điện tử) từ tài khoản của mình
  - Check-like: tiền được lấy từ tài khoản sau khi thanh toán
    - ⇨ Người nộp sẽ gửi một lệnh thanh toán cho người nhận → tiền sẽ bị thu hồi từ tài khoản của người nộp và gửi vào tài khoản của người nhận
    - ⇨ Hóa đơn thanh toán: ví dụ như giấy, phiếu chuyển tiền ngân hàng, hoặc chứng từ điện tử như séc điện tử

18

7. Thanh toán sử dụng thẻ tín dụng

- Là phương pháp phổ biến nhất
  - Các thẻ tín dụng đầu tiên đã được giới thiệu nhiều thập kỷ trước (Diner's Club năm 1949, American Express năm 1958)
- Vật liệu
  - Trong một thời gian dài, hầu hết là thẻ từ có sọc chứa thông tin không được mã hóa, và là các thông tin chỉ đọc
  - Hiện nay, nhiều thẻ thông minh có chứa các thiết bị phần cứng (chip) cung cấp mã hóa và dung lượng lưu trữ lớn hơn

19

7. Thanh toán sử dụng thẻ tín dụng

- **Thẻ tín dụng** *(credit card)* là thẻ chi tiêu trước trả tiền sau, do ngân hàng phát hành.
- Ngân hàng sẽ cấp một số tiền chi tiêu nhất định cho chủ thẻ tín dụng tùy thuộc vào tài chính và lịch sử tín dụng của khách hang, khách hàng có thể chi tiêu trong phạm vi này và cần trả đầy đủ cho ngân hàng mỗi tháng

20

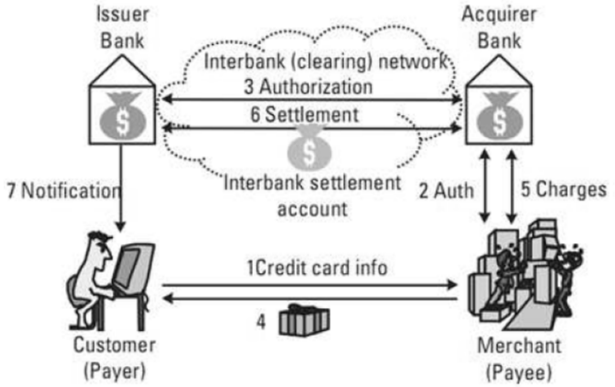
7. Thanh toán sử dụng thẻ tín dụng

21

7. Thanh toán sử dụng thẻ tín dụng

22

Giao dịch thẻ tín dụng đặc trưng



23

Giao dịch thẻ tín dụng đặc trưng

- (1) C gửi M thông tin thẻ tín dụng (ngân hàng phát hành, thời hạn sử dụng, số thẻ)
- (2) M yêu cầu ngân hàng thanh toán A cấp phép
- (3) Ngân hàng thanh toán A kiểm tra với ngân hàng phát hành I, sau đó A thông báo cho M nếu chấp thuận
- (4) M gửi hàng hoá/dịch vụ đã được đặt cho khách hàng C

24

Giao dịch thẻ tín dụng đặc trưng

- (5a) M giải trình chi phí (hoặc gửi một batch các giao dịch) cho A
- (6) Sự thanh toán: A sẽ gửi một yêu cầu thanh toán tới I, I gửi tiền vào một tài khoản thanh toán liên ngân hàng và tính phí số tiền bán hàng vào tài khoản thẻ tín dụng của khách hàng C

25

Giao dịch thẻ tín dụng đặc trưng

- (7) Thông báo
  - Vào khoảng thời gian định kỳ (ví dụ, hàng tháng) ngân hàng phát hành thông báo cho khách hàng C về các giao dịch và chi phí tích lũy
  - Khách hàng C trả những chi phí bằng một số cách khác (ví dụ, đơn hàng ghi nợ trực tiếp, chuyển khoản ngân hàng, séc)
- (5b) Ngân hàng thanh toán A nhận lượng tiền bán hàng từ tài khoản thanh toán liên ngân hàng và ghi vào tài khoản của M (ghi có)

26

8. Tiền điện tử

- Tiền điện tử biểu diễn tiền truyền thống
  - Một đơn vị tiền điện tử thường được gọi là đồng tiền số (e-coin hay digital coin)
  - Đồng tiền số được "đúc" tức là tạo ra bởi các nhà trung gian broker
- Nếu khách hàng C muốn mua đồng tiền số
  - Liên lạc với nhà trung gian môi giới B, đặt hàng một số lượng nhất định của đồng tiền
  - Thanh toán bằng tiền "thật"
  - C có thể mua hàng từ bất kỳ người bán M nào chấp nhận các đồng tiền của B

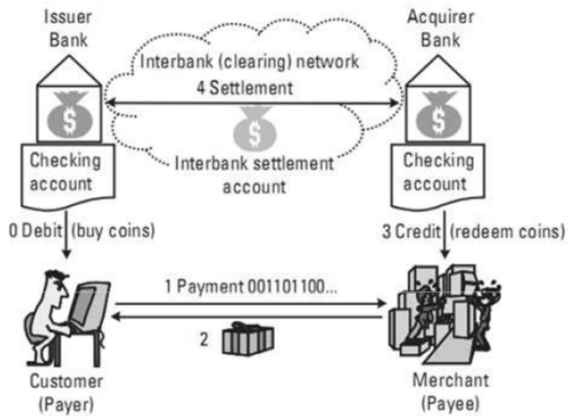
27

8. Tiền điện tử (Tiếp)

- M bù lại các đồng tiền (đã mất) của B mà thu được từ tất cả các khách hàng C
  - B nhận lại các đồng tiền và ghi có vào tài khoản của M bằng tiền thật
- Giao dịch tiền điện tử điển hình
  - Ngân hàng phát hành có thể là các nhà môi giới tại cùng một thời điểm
  - C & M phải có một tài khoản kiểm tra dòng tiền
  - Tài khoản kiểm tra: quá trình luân chuyển, hình thức giữa tiền thật và tiền điện tử

28

Giao dịch tiền điện tử điển hình



Giao dịch tiền điện tử điển hình

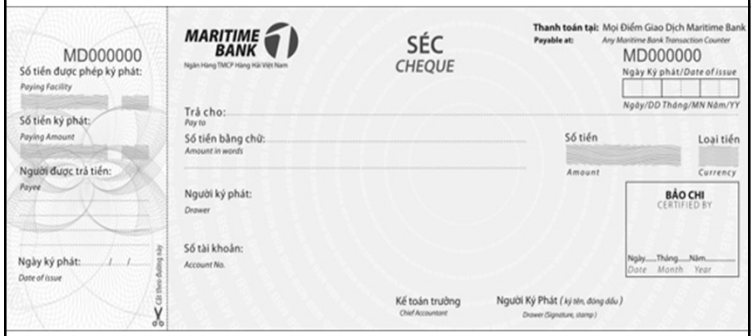
- (0) Rút Coin: Khách hàng C mua đồng tiền và trạng thái kiểm tra tài khoản đang là ghi nợ
- (1) C sử dụng các đồng tiền số để mua hàng trên mạng Internet
- (2) M gửi cho C hàng hóa hoặc dịch vụ
  - Thường dùng để mua các hàng hóa, dịch vụ giá trị thấp
  - Nhà buôn M thường thực hiện đơn hàng của khách hàng C trước hoặc ngay cả khi chưa có thông tin cấp phép thanh toán

Giao dịch tiền điện tử điển hình

- (3) Sự hoàn trả: M sau đó sẽ gửi một yêu cầu tới ngân hàng thanh toán
- (4) Thanh toán: Bằng cách sử dụng một cơ chế thanh toán liên ngân hàng, ngân hàng thanh toán mua lại các đồng tiền tại ngân hàng phát hành và ghi có tài khoản M với số tiền tương đương

9. Séc điện tử

- Séc giấy



Đặc điểm của séc điện tử

- Séc điện tử tương đương với séc giấy truyền thống
- Là tài liệu điện tử có các thông tin sau đây:
  - Số Séc, Tên của người trả tiền
  - Tài khoản Người trả tiền và tên ngân hàng
  - Tên người nhận thanh toán, Số tiền được thanh toán
  - Đơn vị Tiền tệ sử dụng, Ngày hết hạn
  - Chữ ký điện tử của người trả tiền
  - Chứng thực điện tử của Người nhận thanh toán

33

Lợi ích của séc điện tử

- Làm giảm chi phí quản trị của người bán bằng cách nhận được tiền từ người mua nhanh hơn, an toàn hơn và không mất thời gian xử lý giấy tờ.
- Cải thiện hiệu quả của quá trình gửi tiền cho các người bán và các tổ chức tài chính

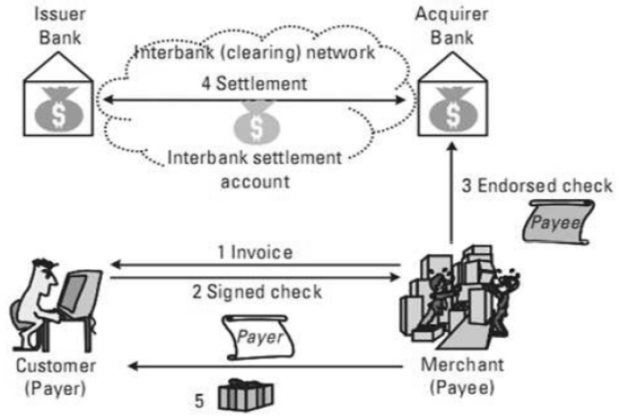
34

Lợi ích của séc điện tử

- Đẩy nhanh tốc độ quá trình thanh toán cho người tiêu dùng
- Cung cấp cho người tiêu dùng có thêm thông tin mua hàng của họ trên báo cáo tài khoản
- Làm giảm việc phải kiểm tra các giá trị động và các con số bị trả lại vì tiền thừa (NSFs)

35

Giao dịch séc điện tử đặc trưng



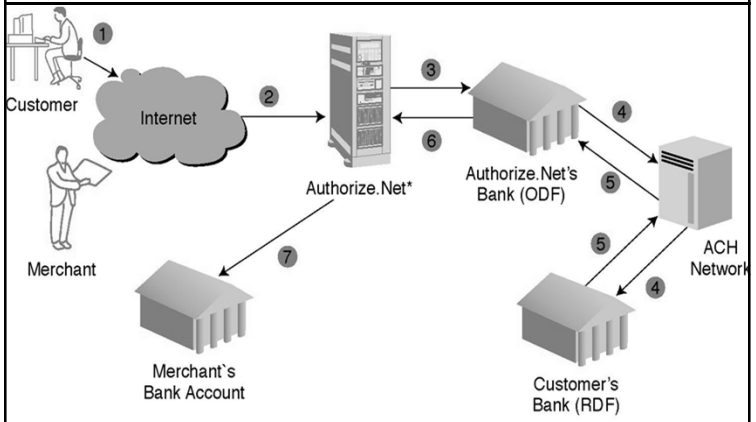
36

Giao dịch séc điện tử đặc trưng

- (1) Khách hàng C đặt đơn hàng/dịch vụ và người bán M sẽ gửi lại hóa đơn điện tử
- (2) Khi thanh toán, C gửi một séc điện tử đã được ký lên đó
- (3) Giống với séc giấy, M chứng thực tờ séc
- (4) Thanh toán: Ngân hàng phát hành và ngân hàng thanh toán sắp xếp chuyển số tiền bán hàng từ tài khoản C vào tài khoản của M
- (5) Vận chuyển/bàn giao

37

Giao dịch séc điện tử sử dụng Authorize.Net



38

10. Ví điện tử

- Ví điện tử là một tài khoản điện tử.
- Ví điện tử được coi như một "ví tiền" của người dùng trên Internet và đóng vai trò như 1 chiếc Ví tiền mặt trong thanh toán trực tuyến, giúp người dùng thực hiện công việc thanh toán các khoản phí trên internet, gửi và nhận tiền một cách nhanh chóng, đơn giản và tiết kiệm cả về thời gian và tiền bạc.

39

10. Ví điện tử

- **Một số loại ví điện tử phổ biến:**
- Trong nước: Ngân lượng , BaoKim, Payoo, MobiVí, MoMo, Smartlink…. Các loại ví điện tử này được phát hành bởi các công ty trong nước và sử dụng phổ biến trong nước.
- Ví điện tử quốc tế: PayPal (phổ biến nhất), AlertPay, WebMoney, Liqpay, Moneybookers….

40

10. Ví điện tử

- Tại các website chấp nhận sử dụng ví tiền điện tử trong thanh toán, người mua sau khi đặt hàng chỉ cần kích vào ví tiền điện tử. Nhập tên và mật khẩu của mình là hoàn tất giao dịch
- Ví điện tử tự động nhập các thông tin cần thiết vào các mẫu trong quy trình mua hàng như địa chỉ giao hàng, số thẻ tín dụng…
- Ví tiền điện tử là một phần mềm được cài đặt trong máy của khách hàng để lưu trữ các thông tin khách hàng
- Khách hàng chỉ sử dụng được dịch vụ này tại các cơ sở chấp nhận ví tiền điện tử tương thích với phần mềm cài đặt trên máy khách hàng

41

10. Ví điện tử

- Chức năng của ví điện tử:
  - Thanh toán trực tuyến: Đóng vai trò như một chiếc ví tiền, ví điện tử có khả năng thanh toán trong các giao dịch mua sắm trực tuyến của người dùng với một số thao tác. Khi thanh toán, thay vì thao tác "rút tiền mặt" ra thanh toán, người dùng sẽ thực hiện thao tác "chuyển tiền" để thực hiện thanh toán.
  - Nhận và chuyển tiền: Là một ví tiền, ví điện tử có khả năng giữ tiền cũng như tham gia các giao dịch chuyển khoản như tài khoản ngân hàng. Người dùng có thể chuyển tiền qua lại giữa các tài khoản ví điện tử hoặc tài khoản ví điện tử và tài khoản ngân hàng.
  - Lưu giữ tiền trên mạng Internet: Khi nạp tiền vào ví, số tiền được sử dụng trong hầu hết các giao dịch thanh toán trực tuyến. Người dùng có thể duy trì số tiền này trong ví và sử dụng khi cần mà không e ngại về vấn đề an toàn và bảo mật của ví

42

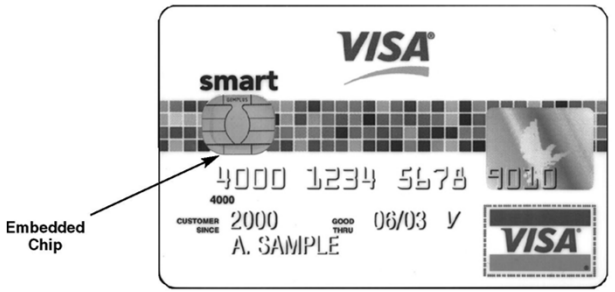
10. Ví điện tử

- Vai trò của ví điện tử
  - Giúp cho các giao dịch được thuận tiện, đơn giản:
  - Người mua thực hiện nhanh chóng công việc thanh toán.
  - Người bán tăng hiệu quả hoạt động bán hàng trực tuyến.
  - Ngân hàng giảm sự quản lý các giao dịch thanh toán từ thẻ khách hàng.
  - Dễ dàng và nhanh chóng chuyển và nhận tiền vượt qua rào cản địa lý.
  - Xã hội giảm bớt lượng tiền mặt trong lưu thông, góp phần ổn định lạm phát.

43

11. Thẻ thông minh

- Thẻ điện tử có chứa một microchip nhúng, cho phép các hoạt động xác định trước, thêm, xóa hay thao tác thông tin trên thẻ



44

11. Thẻ thông minh

- Contact card
  - Một thẻ thông minh có chứa một đĩa vàng nhỏ trên mặt khi được đưa vào trong một đầu đọc thẻ thông minh thì tiếp xúc và chuyển dữ liệu tới và từ microchip nhúng
- Contactless (proximity) card
  - Thẻ thông minh với một ăng-ten nhúng, theo đó dữ liệu và các ứng dụng được truyền đến và đi từ một đơn vị đầu đọc thẻ hoặc thiết bị khác mà không cần tiếp xúc giữa thẻ và đầu đọc thẻ

45

11. Thẻ thông minh

- Smart card reader
  - Kích hoạt và đọc nội dung của các chip trên một thẻ thông minh, thường là chuyển các thông tin tới một hệ thống máy chủ
- Smart card operating system
  - Hệ thống đặc biệt tổ chức quản lý tập tin, tính bảo mật, đầu vào/đầu ra (I/O), thực hiện lệnh và cung cấp một giao diện lập trình ứng dụng (API) cho thẻ thông minh

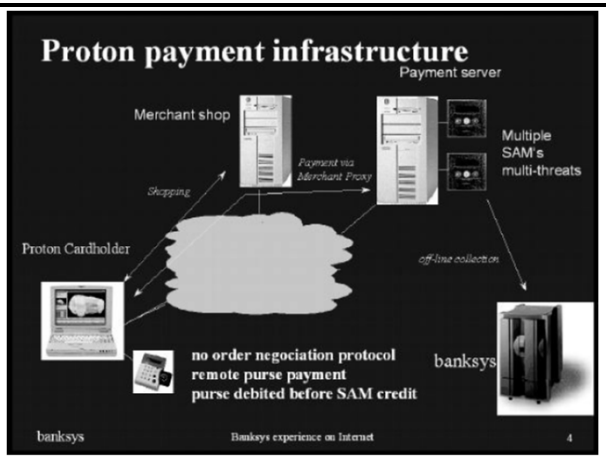
46

Ứng dụng của thẻ thông minh

- Hoạt động mua/bán lẻ
  - Ví điện tử E-purse
    - Ứng dụng thẻ thông minh, nạp tiền từ tài khoản ngân hàng của chủ thẻ lên thẻ chip thông minh
    - Có đặc điểm kỹ thuật của ví điện tử thông thường, tiêu chuẩn điều chỉnh hoạt động và khả năng tương tác của các dịch vụ ví điện tử

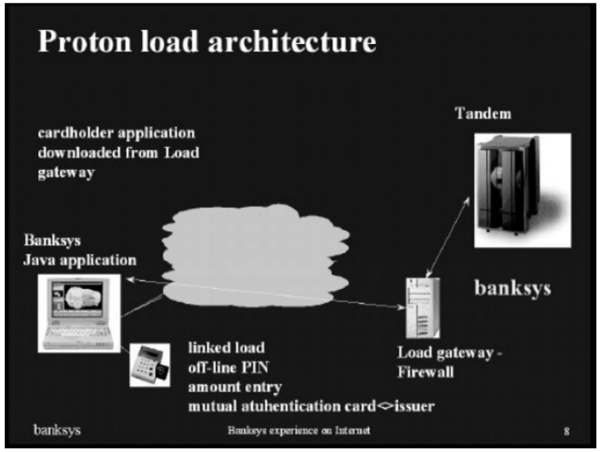
47

E-purse



48

E-purse



49

Ứng dụng của thẻ thông minh

- Transit Giá vé
  - Để loại bỏ sự bất tiện của nhiều loại vé được sử dụng trong các phương tiện giao thông công cộng
  - Thực hiện hệ thống bán vé bằng thẻ thông minh

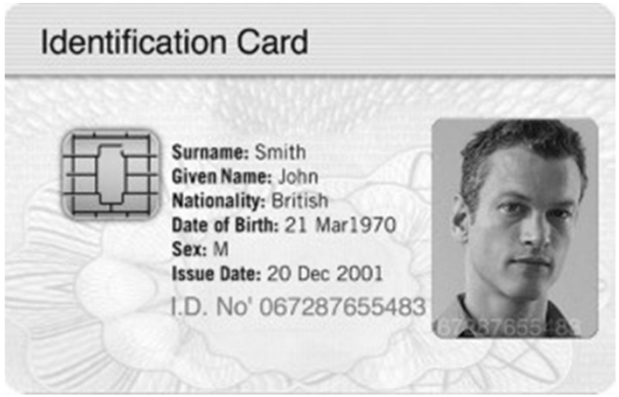
50

Ứng dụng của thẻ thông minh

- Chứng thực điện tử (E-Identification)
  - Lưu trữ thông tin cá nhân: hình ảnh, nhận dạng sinh trắc học, chữ ký số, và các phím bảo mật cá nhân, thẻ thông minh đang được sử dụng trong một loạt các ứng dụng xác định, kiểm soát truy cập, và xác thực
  - eID
  - eDriver's License
  - ePassport
  - eHealth Card
  - eEmployee Card
  - eDigital Signature Card
  - eCitizen Card

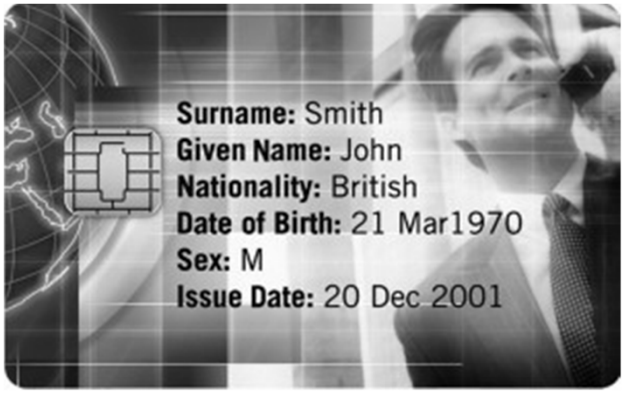
51

eID



52

eEmployee Card



53

ePassport

54

Ứng dụng thẻ thông minh trong chăm sóc y tế

55

Ứng dụng thẻ thông minh trong chăm sóc y tế

- Lưu trữ thông tin y tế quan trọng trong trường hợp khẩn cấp
- Ngăn chặn các bệnh nhân nhận đơn thuốc từ các bác sĩ khác nhau
- Xác minh danh tính của bệnh nhân và bảo hiểm
- Đẩy nhanh quy trình giường bệnh hoặc các tình huống khẩn cấp

56

Ứng dụng thẻ thông minh trong chăm sóc y tế (Tiếp)

- Cung cấp cho học viên y tế có quyền truy cập an toàn vào lịch sử y tế của bệnh nhân hoàn chỉnh
- Đẩy nhanh quá trình thanh toán và tuyên bố
- Cho phép bệnh nhân để truy cập các hồ sơ y tế của họ qua Internet

57

Thẻ thông minh an ninh

- Thẻ thông minh lưu trữ hoặc cung cấp truy cập vào tài sản có giá trị hoặc thông tin nhạy cảm
- Phải được đảm bảo an toàn, chống trộm cắp, lừa đảo, hoặc sử dụng sai
- Khả năng để thực hiện hack vào một thẻ thông minh thuộc phân loại tấn công “lớp 3”, đồng nghĩa với việc chi phí liên quan đến thẻ vượt xa những lợi ích mang lại

58

Thẻ lưu trữ giá trị (Stored-value Card)

- Một thẻ có giá trị tiền tệ được nạp vào nó và thường có thể chuyển đổi

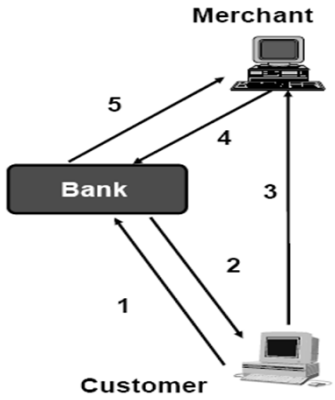
59

12. Tiền mặt điện tử (Electronic Cash)

- Thuận lợi căn bản
  - Sử dụng trong các giao dịch mua bán vừa và nhỏ
  - Thanh toán các mặt hàng ít hơn $10
  - Phí giao dịch của thẻ tín dụng sẽ là trở ngại với những giao dịch buôn bán nhỏ
  - Thực hiện thanh toán Micropayments cho các hạng mục chi phí ít hơn 1$

60

Giao thức tiền mặt điện tử cơ bản



61

Giao thức tiền mặt điện tử cơ bản

- Các bước cơ bản của giao thức
  - (1) C mua/trừ tiền mặt từ Ngân hàng
  - (2) B → C: đồng xu điện tử, khi tính số tiền yêu cầu + lệ phí
  - (3) C → M: đồng xu điện tử
  - (4) M → B: yêu cầu kiểm tra tính hợp lệ của đồng xu điện tử
  - (5) B → M: Xác thực giá trị đồng tiền
  - Các bên tiếp tục hoàn tất giao dịch cùng với người bán
    - ⇨ Tiền mặt điện tử hiện tại gửi vào ngân hàng phát hành khi hàng/dịch vụ được chuyển giao

62

Những vấn đề phát sinh với tiền mặt điện tử

- Đồng xu điện tử chỉ được chi tiêu một lần
- Người dùng thích sự nặc danh giống như với tiền mặt thực tế
  - Các biện pháp an ninh phải được thực hiện để ngăn chặn việc làm giả đồng tiền
- Dễ chia nhỏ và thuận tiện
- Giao dịch phức tạp (phải kiểm tra với Ngân hàng)
- Vấn đề nguyên tử

63

Hai phương thức lưu trữ

- On-line
  - Người dùng không có sở hữu cá nhân với e-coins
  - Do bên thứ ba đáng tin cậy chẳng hạn như ngân hàng trực tuyến nắm giữ tài khoản tiền mặt của khách hàng
- Off-line
  - Người dùng có thể giữ e-coins trong thẻ thông minh hoặc phần mềm ví điện tử
  - Sự gian lận và sử dụng 2 lần đòi hỏi các kỹ thuật chống trộm đặc biệt

64

Thuận lợi và bất lợi của tiền mặt điện tử

- Thuận lợi
  - Hiệu quả hơn
  - Chi phí giao dịch thấp hơn
  - Thực hiện được với tất cả mọi người, không giống với thẻ tín dụng (yêu cầu cấp quyền hạn đặc biệt)
- Bất lợi
  - Thuế
  - Nạn rửa tiền
  - Dễ bị làm giả

65

Thanh toán Micropayment

- Thay thế cho phương tiện tiền mặt điện tử
- Rẻ hơn, không quá đắt để quản lý
- Quay vòng nhanh hơn
- Dễ dàng đếm, kiểm soát, xác thực
- Giá trị giao dịch thấp
- Chi phí giao dịch thấp

66

Thanh toán Micropayment

- Thích hợp nhất với những giao dịch nhỏ (nhỏ hơn 1$)
  - Đồ uống
  - Cuộc gọi điện thoại
  - Lệ phí cầu đường, vận chuyển, đỗ xe
  - Sao chép, nội dung Internet, Xổ số, cờ bạc

67

Thanh toán Micropayment từ xa

- Bên mua là từ xa so với bên bán
- Không thể chèn thẻ vào máy của nhà cung cấp
- Không có hàng hoá vật lý, chỉ có hàng hóa thông tin
- Khi sử dụng hệ thống micropayment, hàng hoá phải có giá rẻ, ví dụ như 0.01$

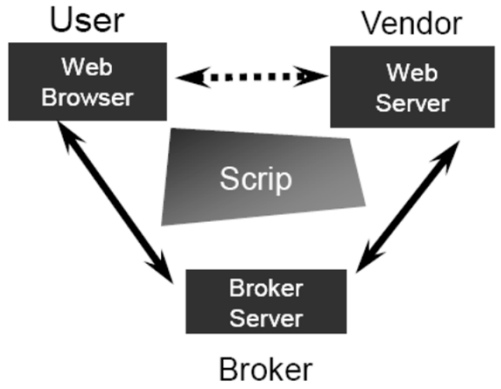
68

Thanh toán Micropayment từ xa (Tiếp)

- Thanh toán truyền thống là quá đắt
  - Thuê bao điện thoại, thẻ tín dụng, séc, ACH hoặc PayPal
  - Ví dụ như thanh toán để xem các trang web, giá cổ phiếu, tin tức, báo cáo thời tiết, thư mục tra cứu
- Tính năng yêu cầu
  - Dịch vụ ngay lập tức
  - Giao dịch có giá rẻ (1coins) nhưng trong 1 số lượng giao dịch lớn
  - Lợi nhuận hợp lý cho nhà cung cấp dịch vụ thanh toán

69

Thanh toán Micropayment từ xa (Tiếp)



70

Thanh toán Micropayment từ xa (Tiếp)

- Người sử dụng (người mua)
- Các nhà cung cấp (bên bán)
- Môi giới (trung gian)
  - Phát hành ‘scrip’ (là loại tiền ảo cho người sử dụng)
  - Mua lại scrip từ các nhà cung cấp để lấy tiền thật
- Các giả định
  - Quan hệ User-Broker là quan hệ lâu dài
  - Quan hệ Vendor-Broker là lâu dài
  - Quan hệ User-Vendor là ngắn hạn

71

Hiệu quả của Micropayment

- Các nhà cung cấp cần phải xử lý thời điểm có nhiều giao dịch (2500 giao dịch/giây)
- Sử dụng công cụ bảo mật có chi phí thấp
  - Mật mã khóa công khai là đắt tiền
  - Cần giảm thiểu lưu lượng truy cập Internet
    - Máy chủ phải được nâng cấp
    - Nhiều máy chủ yêu cầu, hàng đợi lâu hơn, thất thoát gói tin đến chậm
    - Hủy bỏ các broker khỏi quy trình (chỉ có người sử dụng + vendor)

72

Hiệu quả của Micropayment (Tiếp)

- Đối với các khoản thanh toán nhỏ, sự hoàn hảo là không cần thiết
  - Không phải là vấn đề lớn, nếu mất đi một micropayment
  - Cần đảm bảo việc gian lận micropayment là thấp

73

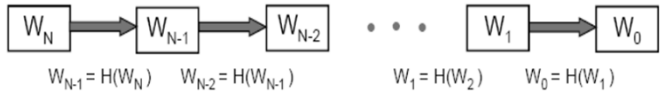
Khái niệm Payword

- Payword là hệ thống thanh toán cho các giao dịch giá trrị nhỏ.
- Payword thích hợp cho các thanh toán lặp lại nhiều lần cùng với một nhà cung cấp.
- Phương thức thanh toán an toàn sử dụng hàm băm
  - Như một công cụ mã hoá light-weight, các hàm băm dễ dàng tính toán, thuộc tính 1 chiều của nó giúp bảo vệ chống lại việc ăn cắp các giá trị nhỏ

74

Khái niệm Payword

- Giả sử chúng ta cần N "đồng xu"
  - Bắt đầu với một số ngẫu nhiên W_N
  - Băm N lần để hình thành W_0



  - N con số này sẽ được sử dụng như là "đồng xu", hoặc payword, mỗi đồng có giá trị một đơn vị
  - Người bán hàng nhận W_0 để bắt đầu

75

Payword

- Dựa trên những chuỗi "payword" được chấp nhận bởi các nhà cung cấp để mua hàng
- Đầu tiên, người dùng xác thực với nhà môi giới của mình một chữ ký xác minh, trả tiền thật cho các paywords
- Người dùng thiết lập với nhà môi giới (Broker) một chuỗi liên kết các paywords được dùng với một nhà cung cấp (Vendor) cụ thể

76

Payword

- Liên kết được sử dụng để chứng thực các paywords có thể được kết hợp, vì vậy chi phí rất rẻ
- Người dùng trả tiền cho nhà cung cấp bằng cách tiết lộ paywords cho nhà cung cấp
- Chi phí biên của một khoản thanh toán: một tính toán hash

77

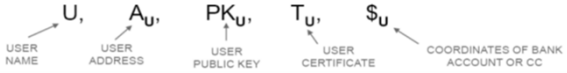
Payword

- Người dùng thiết lập tài khoản Payword với một nhà môi giới (trả tiền thật)
  - Nhà Môi giới phát hành cho người dùng 1 thẻ "ảo" (chứng nhận)
    - Tên nhà Môi giới, tên người dùng, địa chỉ IP người sử dụng, khóa công khai người sử dụng
  - Chứng nhận xác thực người dùng với nhà cung cấp
  - Người sử dụng tạo ra chuỗi payword (độ dài điển hình là: 100 đơn vị) đặc trưng cho một nhà cung cấp

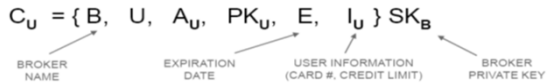
78

Mua Payword

- Người dùng "thăm" nhà môi giới thông qua kênh an toàn (ví dụ như SSL), cung cấp sự kết hợp với khoản ngân hàng hoặc thẻ tín dụng:



- Nhà trung gian môi giới phát hành 1 thẻ thuê bao



- Nhà cung cấp chỉ gửi hàng tới A_U

79

Thực hiện thanh toán

- Cam kết một chuỗi payword = lời hứa của người sử dụng trả cho nhà cung cấp cho tất cả paywords được đưa ra bởi người sử dụng trước khi hết hạn sử dụng
  - N = giá trị trong các jetons cần thiết cho việc mua bán (1 payword = 1 jeton)
  - W_N = payword cuối cùng, giá trị ngẫu nhiên đã chọn bởi người sử dụng

80

Thực hiện thanh toán

- Tạo ra chuỗi payword ngược bằng cách băm W_N

$$W_{N-1} = H(W_N);\ W_{N-2} = H(W_{N-1}) = H(H(W_N))$$

$W = \{ W_0, W_1, \ldots W_{N-1}, W_N \}$ ← CAN EASILY COMPUTE THIS WAY
→ DIFFICULT TO COMPUNTE THIS WAY

- Người dùng "cam kết" chuỗi này với vendor và gửi

M IS VENDOR SPECIFIC AND USER-SPECIFIC → $M = \{ V, C_U, W_0, D, I_M \} SK_U$ [EXPENSIVE: REQUIRES DIGITAL SIGNATURE]

(NO USE TO ANYONE ELSE)
VENDOR NAME
"FIRST" PAYWORD
EXPIRATION DATE OF COMMITMENT
EXTRA INFORMATION (VALUE OF CHAIN)
USER PRIVATE KEY

81

Thực hiện thanh toán (Tiếp)

- Người bán hàng có thể sử dụng PK_U và PK_B để đọc các cam kết để biết rằng U hiện đang được uỷ quyền để chi tiêu paywords
- Người sử dụng "chi tiêu" paywords với các nhà cung cấp theo thứ tự $W_1, W_2, \ldots, W_N$
- Để chi tiêu payword W_i, người sử dụng gửi các nhà cung cấp mã thông báo unsigned $P = \{W_i, i\}$

82

Thực hiện thanh toán (Tiếp)

- Để xác minh rằng P là hợp pháp, nhà cung cấp thực hiện băm i lần để có được W_0, nếu phù hợp với W_0 trong cam kết, thanh toán sẽ thực hiện tốt
- Nếu V lưu trữ các giá trị payword cuối cùng từ U, chỉ cần băm 1 lần (nếu lần cuối băm là W_i, khi nhà cung cấp nhận được W_{i+1}, có thể băm nó một lần và so sánh với W_i)
- P không cần phải ký kết bởi vì hàm băm là một chiều

83

Thanh toán với Payword

- Ngay cả khi vendor không có mối quan hệ với nhà môi giới B, vẫn có thể xác minh paywords của người sử dụng (chỉ cần khóa công khai của nhà môi giới)
- Đối với vendor để có được tiền từ B đòi hỏi phải có mối quan hệ
- Vendor gửi môi giới B yêu cầu bồi hoàn cho các người dùng gửi paywords với M, W_L (giá trị payword cuối cùng nhận được bởi vendor)

84

Thanh toán với Payword

- Broker kiểm tra từng cam kết sử dụng PK_U và thực hiện L băm để đi từ W_L tới W_0
- Broker trả tiền cho V, tập hợp các cam kết của U và các hóa đơn thẻ tín dụng của U hoặc ghi nợ tiền từ tài khoản ngân hàng của U

85

Thuộc tính của thanh toán Payword

- Thanh toán và xác thực bởi nhà cung cấp là offline (không sử dụng thẩm quyền đáng tin cậy)
- Thanh toán thẻ P không tiết lộ hàng
- Gian lận bằng cách sử dụng (phát hành paywords mà không phải trả tiền cho chúng) sẽ được phát hiện bởi nhà môi giới, mất mát nhỏ
- Vendor giữ hồ sơ của paywords chưa hết hạn để bảo vệ chống lại phát hành lại

86

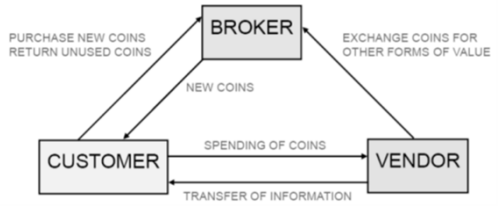
Ý tưởng chính

- Nhanh chóng và có chi phí thấp
- Thiếu các tính năng của hệ thống thanh toán các giá trị cao hơn
- Sử dụng hàm băm thay vì mã hóa
- Thành phần của Micropayment: người mua, người bán, môi giới
- Payword người dùng tạo ra đồng tiền riêng của mình
- Gian lận không phải là một vấn đề nghiêm trọng với micropayments

87

MicroMint

- Brokers sản xuất "đồng xu" có vòng đời ngắn, bán tiền xu cho người sử dụng
- Người sử dụng phải trả nhà cung cấp bằng tiền xu
- Các nhà cung cấp trao đổi tiền xu với các nhà môi giới bằng tiền "thật" bỏ ra



88

Đúc xu trong MicroMint

- Ý tưởng: làm cho đồng tiền dễ dàng để xác minh, nhưng khó khăn để tạo ra (vì vậy không có lợi khi làm giả)
- Trong MicroMint, đồng xu được biểu diễn bởi đụng độ hash-function, các giá trị x, y sao cho H (x) = H (y)

89

Đúc xu trong MicroMint

- Nếu H (•) trả kết quả là một giá trị băm n-bit, chúng ta phải thử $2^{n/2}$ giá trị của x để tìm một đụng độ 2-chiều đầu tiên
- Thử $c*2^{n/2}$ giá trị của x để có c^2 đụng độ
- Việc tạo ra các đụng độ trở nên rẻ hơn sau khi một trong những đụng độ đầu tiên được tìm thấy

90

Đúc xu trong MicroMint

- Một đụng độ k-chiều là một tập hợp $\{x_1, x_2, . . , x_k\}$ với $H (x_1) = H (x_2) = . . = H (x_k)$
- Phải mất khoảng $2^{n(k-1)/k}$ giá trị của x để tìm một đụng độ k chiều
- Phép thử $c•2^{n(k-1)/k}$ giá trị của x sản xuất khoảng c^k đụng độ
- Nếu k>2, việc tìm kiếm một đụng độ đầu tiên là chậm, nhưng chuỗi đụng độ sau đó sẽ nhanh chóng

91

Đúc xu trong MicroMint

- Nếu một đụng độ k-chiều $\{x_1, x_2, ... , x_k\}$ biểu diễn cho một đồng xu, dễ dàng được xác nhận bằng cách tính $H (x_1), H (x_2). . , H (x_k)$
- Một người môi giới có thể dễ dàng tạo ra 10 tỷ đồng tiền xu mỗi tháng bằng cách sử một cơ chế

92

Bán xu MicroMint

- Môi giới tạo ra 10 tỷ đồng tiền và các lưu trữ (x, H (x)) cho mỗi đồng xu, với thời gian hiệu lực là một tháng
- Các hàm H thay đổi ở đầu mỗi tháng
- Broker bán đồng xu $\{x_1, x_2, . . , x_k.\}$ cho người sử dụng để lấy tiền "thật", ghi lại thông tin những người mua xu
- Vào cuối tháng, người sử dụng đổi lại những đồng xu chưa tiêu để lấy xu mới

93

Chi tiêu xu MicroMint

- Người sử dụng gửi vendor một đồng xu $\{x_1, x_2, . . , x_k\}$
- Người bán hàng kiểm tra tính hợp lệ bằng cách kiểm tra $H(x_1) = H(x_2) = . . = H(x_k)$ (k phép tính băm)
- Nếu hợp lệ nhưng những đồng xu sử dụng 2 lần (trước đây được sử dụng với một nhà cung cấp khác) không thể được phát hiện vào thời điểm này
- Vào cuối ngày, vendor gửi tiền xu tới broker
- Broker xác minh đồng tiền, kiểm tra tính hợp lệ, kiểm tra double spending, trả tiền cho vendor

94

Phát hiện giả mạo MicroMint

- Một đồng xu giả mạo là đụng độ k chiều $\{x_1, x_2, . . , x_k\}$ dưới hàm H (•) là không được đúc bởi broker
- Người bán hàng không có thể xác định điều này trong thời gian thực
- Quy mô nhỏ nên việc giả mạo là không khả thi
- Giả mạo tiền trở nên không hợp lệ sau một tháng
- Giả mạo không thể bắt đầu trước khi hàm băm mới được công bố

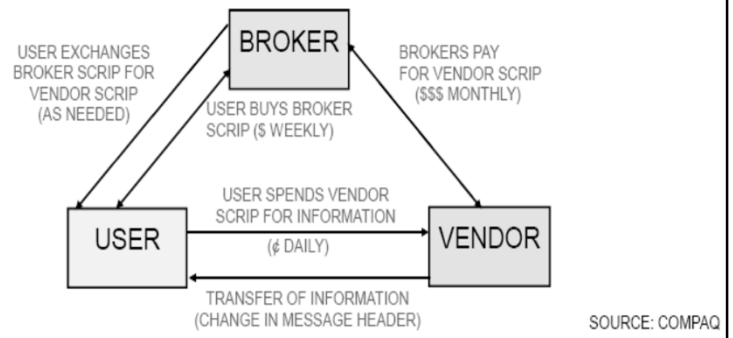
95

Millicent

- Vendor sản xuất "scrip" cùng thông tin xác định vendor, bán cho brokers để thu tiền thật
- Broker bán scrip của nhiều vendors cho nhiều người sử dụng
- Scrip được trả trước: cam kết các dịch vụ tương lai từ nhà cung cấp
- Người sử dụng "chi tiêu" scrip với vendors, ghi nhận thay đổi

96

Millicent



97

Millicent

- **Broker**
  - Phát hành broker scrip cho người sử dụng
  - Trao đổi broker scrip với vendor scrip
  - Giao tiếp với hệ thống ngân hàng
  - Thu thập ngân quỹ từ người sử dụng
  - Trả tiền cho vendors (ít hoa hồng)

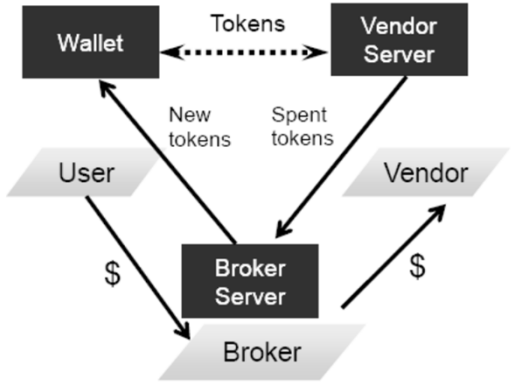
98

Millicent

- **User**
  - Mua broker scrip từ brokers
  - Chi tiêu bằng cách lấy scrip có thông tin nhà cung cấp cụ thể từ broker
- **Vendor**
  - Bán scrip cho brokers
  - Chấp nhận vendor scrip từ người sử dụng
  - Gửi những thay đổi cho người dùng trong vendor scrip

99

Thành phần của Millicent



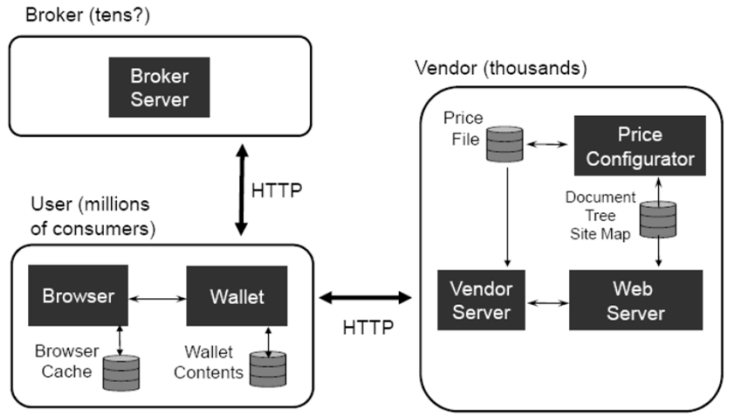
100

Thành phần của Millicent

- Ví điện tử
  - Tích hợp với trình duyệt như là một "proxy"
  - Giao diện người dùng (nội dung, sử dụng)
- Phần mềm của vendor
  - Dễ dàng để tích hợp như là một web relay
  - Tiện ích cho quản lý giá
- Phần mềm của broker
  - Xử lý tiền thật

101

Kiến trúc của Millicent



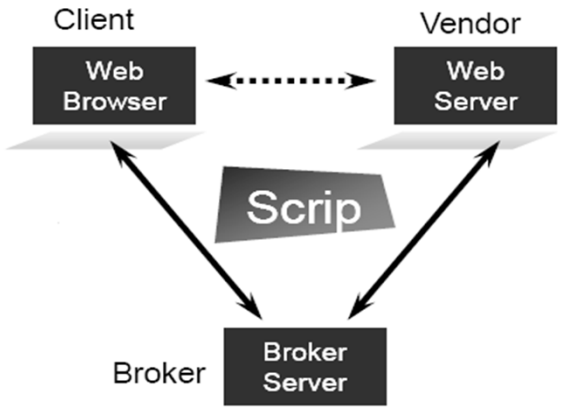
102

Xác thực scrip Millicent

- Mã thông báo kèm theo các yêu cầu HTTP
- Scrip không thể được:
  - Tiêu hai lần
  - Làm giả
  - Bị đánh cắp
- Scrip được xác nhận
  - Thông qua vendor
  - Chi phí tính toán thấp
  - Không cần kết nối mạng
  - Không cần CSDL tìm kiếm

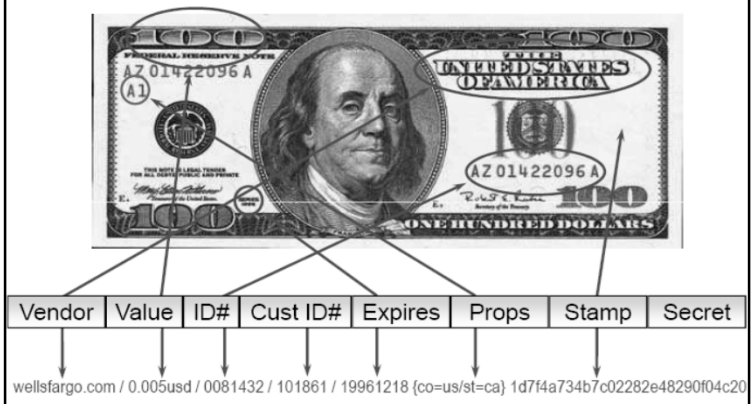
103

Xác thực scrip Millicent



104

Scrip Millicent



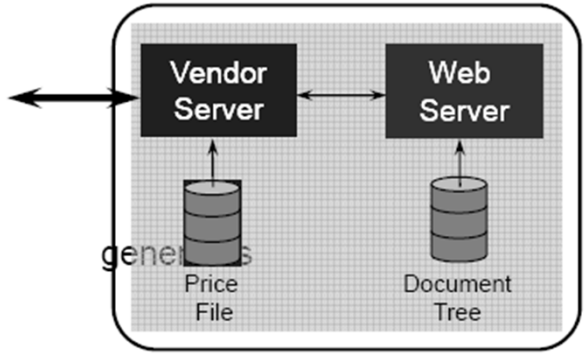
105

Máy chủ của vendor

- Máy chủ nhà cung cấp hoạt động như một proxy cho máy chủ Web thực
- Máy chủ nhà cung cấp xử lý tất cả các yêu cầu
  - Millicent relay web server
  - Máy chủ
- Xử lý Millicent
  - Xác nhận scrip và tạo ra thay đổi
  - Bán bản đăng ký
  - Xử lý replay, cash-out, và hoàn lại tiền

106

Vendor Site



107

Ý tưởng chính

- Các hệ thống micropayment phải nhanh và rẻ
- Thiếu các tính năng của hệ thống thanh toán giá trị cao hơn
- Sử dụng hàm băm thay vì mật mã
- Gồm các bên: người mua, người bán, môi giới
- Mô hình Micromint đúc tiền xu
  - Chi phí cao để ngăn chặn hàng giả
- Gian lận không phải là một vấn đề nghiêm trọng với micropayments

108